WHAT IS CLAIMED IS:

1. A public key certificate issuing system comprising:

a certificate authority for issuing a public key certificate used by an entity; and

a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority;

wherein said certificate authority, having a plurality of signature modules each executing a different signature algorithm, selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

2. A public key certificate issuing system according to claim 1, wherein said certificate authority has a plurality of signature modules and a certificate authority server for outputting a signature processing request to said plurality of signature modules;

wherein said certificate authority server receives said public key certificate issuance request from said

registration authority, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module; and

wherein each of said plurality of signature modules attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server.

3. A public key certificate issuing system according to claim 1, wherein said certificate authority has a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a signature algorithm specific to each of said registration authorities; and

wherein, given a public key certificate issuance request from any registration authority, said certificate authority selects the signature module associated with the relevant signature algorithm based on said registration authority management data.

4. A public key certificate issuing system according to claim 3, wherein said registration authority

management data include key length and parameter information applicable to signatures.

5. A public key certificate issuing system according to claim 3, wherein said registration authority management data include signature module identification information applicable to signatures.

6. A public key certificate issuing system according to claim 1, wherein said registration authority transmits signature algorithm designation information along with said public key certificate issuance request to said certificate authority; and

wherein said certificate authority, based on said signature algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated signature algorithm.

7. A public key certificate issuing system according to claim 6, wherein said signature algorithm designation information includes key length and parameter information applicable to signatures.

8. A public key certificate issuing system according to claim 1, wherein said certificate authority has a verification key database which stores keys for signature verification in association with each of said

plurality of signature modules; and

wherein said certificate authority verifies signatures generated by each of said plurality of signature modules.

9. A public key certificate issuing system according to claim 1, wherein said certificate authority uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate.

10. A public key certificate issuing system according to claim 1, wherein said certificate authority selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation.

11. A public key certificate issuing system according to claim 1, wherein said certificate authority and said registration authority each have a signature module structure management table which associates signature algorithm identifiers with identifiers of said plurality of signature modules;

wherein said registration authority issues to said certificate authority a public key certificate issuance request designating a signature algorithm identifier in

accordance with said signature module structure management table; and

wherein said certificate authority, upon receipt of said signature algorithm identifier from said registration authority, selects the signature module applicable to the received identifier from said signature module structure management table.

12. A public key certificate issuing system according to claim 1, wherein at least part of said plurality of signature modules have a common signature key stored therein.

13. A public key certificate issuing system according to claim 1, wherein a plurality of signature algorithms are executed by each of said plurality of signature modules.

14. A public key certificate issuing method for use with a certificate authority for issuing a public key certificate used by an entity, and with a registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority, the method comprising the steps of:

causing said certificate authority selects, from

among a plurality of signature modules each executing a different signature algorithm, at least one of the signature modules in accordance with said public key certificate issuance request from said registration authority; and

causing the selected signature module to attach a digital signature to message data constituting a public key certificate.

15. A public key certificate issuing method according to claim 14, further comprising the steps of:

causing a certificate authority server to receive a public key certificate issuance request from said registration authority;

causing said certificate authority server to select at least one of said plurality of signature modules in response to said public key certificate issuance request; and

causing said certificate authority server to output a signature processing request to the selected signature module.

16. A public key certificate issuing method according to claim 14, wherein said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on

a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a signature algorithm specific to each of said registration authorities.

17. A public key certificate issuing method according to claim 14, wherein said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on signature algorithm designation information received along with said public key certificate issuance request.

18. A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to verify signatures generated by each of said plurality of signature modules.

19. A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to use at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate.

20. A public key certificate issuing method according to claim 14, further comprising the step of causing said certificate authority to select at least two

of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation.

21. A public key certificate issuing method according to claim 14, wherein said certificate authority and said registration authority each have a signature module structure management table which associates signature algorithm identifiers with identifiers of said plurality of signature modules, said public key certificate issuing method further comprising the steps of:

causing said registration authority to issue to said certificate authority a public key certificate issuance request designating a signature algorithm identifier in accordance with said signature module structure management table; and

causing said certificate authority, upon receipt of said signature algorithm identifier from said registration authority, to select the signature module applicable to the received identifier from said signature module structure management table.

22. A public key certificate issuing method according to claim 14, further comprising the step of

having a plurality of signature algorithms executed by each of said plurality of signature modules.

23. A digital certification apparatus for constituting a certificate authority which issues a public key certificate used by an entity:

wherein said digital certification apparatus, having a plurality of signature modules each executing a different signature algorithm, selects at least one of said plurality of signature modules in accordance with a public key certificate issuance request received from outside, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate.

24. A digital certification apparatus according to claim 23, further comprising a plurality of signature modules and a certificate authority server for outputting a signature processing request to said plurality of signature modules;

wherein said certification authority server receives said public key certificate issuance request, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module; and

wherein each of said plurality of signature modules attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server.

25. A digital certification apparatus according to claim 23, further comprising a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with a signature algorithm specific to each of said registration authorities;

wherein, given a public key certificate issuance request from any registration authority, said digital certification apparatus selects the signature module associated with the relevant signature algorithm based on said registration authority management data.

26. A digital certification apparatus according to claim 25, wherein said registration authority management data include key length and parameter information applicable to signatures.

27. A digital certification apparatus according to claim 25, wherein said registration authority management data include signature module identification information

applicable to signatures.

28. A digital certification apparatus according to claim 23, wherein said digital certification apparatus, based on signature algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated signature algorithm.

29. A digital certification apparatus according to claim 28, wherein said signature algorithm designation information includes key length and parameter information applicable to signatures.

30. A digital certification apparatus according to claim 23, further comprising a verification key database which stores keys for signature verification in association with each of said plurality of signature modules;

wherein said digital certification apparatus verifies signatures generated by each of said plurality of signature modules.

31. A digital certification apparatus according to claim 23, wherein said digital certification apparatus uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate.

32. A digital certification apparatus according to claim 23, wherein said digital certification apparatus selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation.

33. A digital certification apparatus according to claim 23, further comprising a signature module structure management table which associates signature algorithm identifiers with identifiers of said plurality of signature modules;

wherein said digital certification apparatus, upon receipt of a signature algorithm identifier along with said public key certificate issuance request, selects the signature module applicable to the received identifier from said signature module structure management table.

34. A digital certification apparatus according to claim 23, wherein at least part of said plurality of signature modules have a common signature key stored therein.

35. A digital certification apparatus according to claim 23, wherein a plurality of signature algorithms are executed by each of said plurality of signature modules.

36. A program storage medium which stores a

computer program executed by a computer system in carrying out public key certificate issuance processing to issue a public key certificate for use by an entity, said computer program comprising the steps of:

selecting, from among a plurality of signature modules each executing a different signature algorithm, at least one of the signature modules in accordance with a public key certificate issuance request; and

causing the selected signature module to attach a digital signature to message data constituting a public key certificate.